Information Warfare
How do hackers hack?

Doug Jacobson

Information Assurance Center

www.iac.iastate.edu

October 24th, 2002

Today

- How bad is it?
- Steps used in hacking
- IA at ISU

How do hackers hack?

- The key to hacking is information
- From the *Art of War by Sun Tzu*
  - By discovering the enemy's dispositions and remaining invisible ourselves, we can keep our forces concentrated, while the enemy's must be divided.
  - Knowledge of the enemy's dispositions can only be obtained from other men.

“Cyber Terrorism”

News Stories…

- Hackers post graffiti on CIA web page
- Hackers publish credit card numbers stolen from an online vendor
- Cyber Warfare now SOP in military offensive tactics
- Hackers develop extensive network to exchange passwords
- Coordinated attacks using public domain hack tools cripple major e-commerce sites
- Existing software tools are largely ineffective
- Internet infrastructure (DNS) attacked by DDoS

How Big of a Problem is this?

- Recent survey of over 1600 professionals
  - 59% of sites using E-commerce reported at least one security breach
  - 52% of sites not using E-commerce reported at least one security breach
- **Most** security breaches are not reported
- Breaches used to be an annoyance; now they are million dollar losses

The Cost of Security Breeches

2001 Computer Crime and Security Survey (Computer Security Institute + FBI)

538 US security workers polled:

- 85% detected break-in in last year
- 64% suffered financial loss
- Of those reporting(186), total loss was $378M (stolen secrets, fraud)

Most break-ins are not reported

Some Experts Say We Are At War…

- US intellectual property is being data-mined
- Civilian infrastructure is at risk
  - Power grid
  - Water & Telecommunications
  - Ability to do commerce over the web
  - Telemedicine applications
  - Law enforcement

Core Problems

We have millions of systems out there in which:

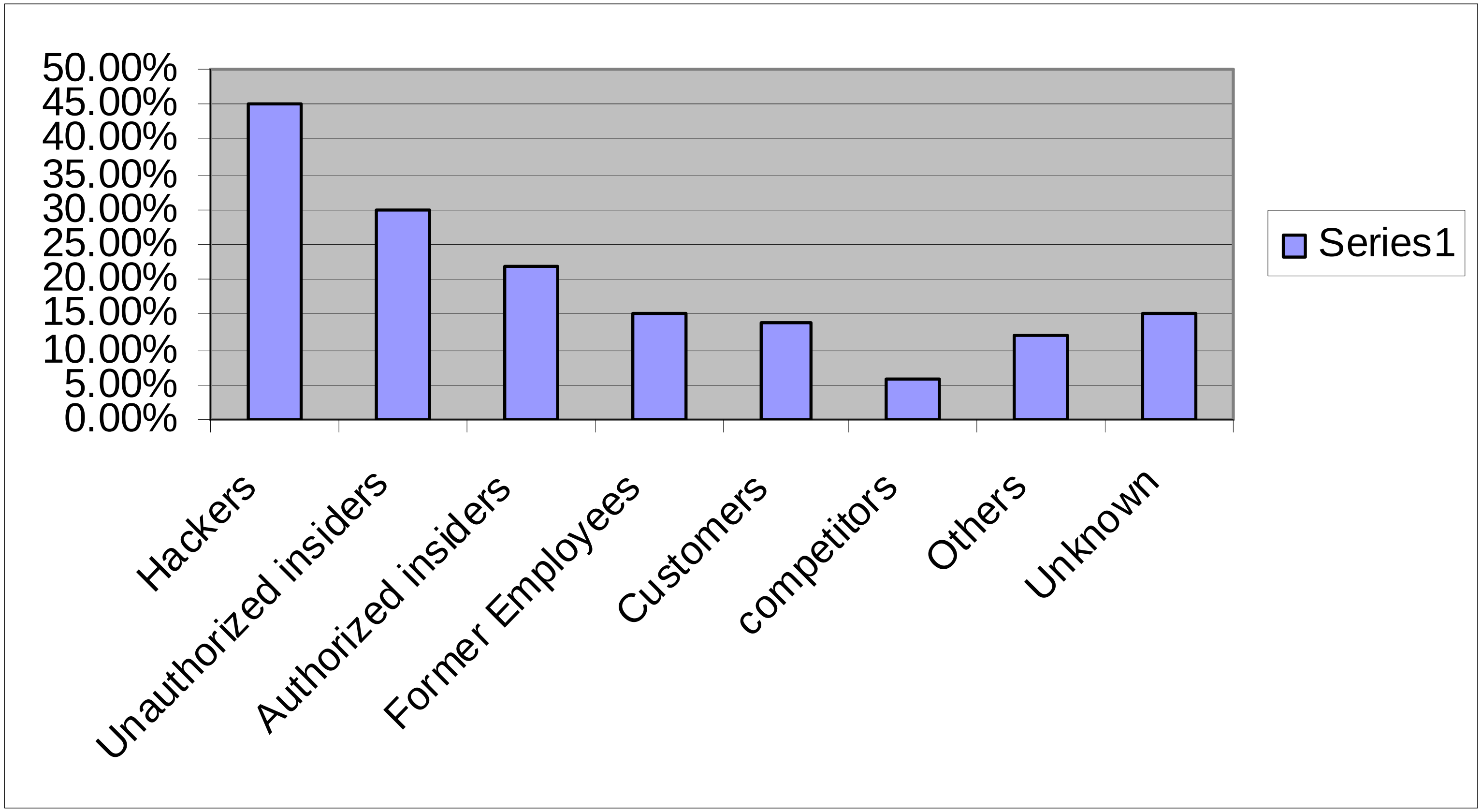
- Interoperability is more important than security
- Poorly designed or tested software
- Users do not hold vendors accountable for developing secure systems and software
- Social/people problem

Who are they and how hard is it?

- Script kiddies
- Hackers
- Professionals
- Nation states
- Search of google (hacking tools) = 277,000 hits

Who are they?

Intruders (Information week 02-11-02)



Why should I Care?

- National loss
  - Economic
  - Terrorism
- Personal loss of
  - Privacy
  - Money

What would they want from me?

- Your computer
- Your network
- Your data
- Your identity
- Nothing, it just fun

Steps in hacking

1. Find the targets
2. Locate the target’s assets
3. Find any vulnerabilities in the assets
4. Gain access
5. Increasing access
6. Gather data
7. Making a backdoor
8. Cover tracks

- Trashing it or taking it off-line

Find the targets

- Can be done with the knowledge of the target
- Random targets (low hanging fruit)
- Specific target
  - Jump off point for other attacks
  - Political statement
  - Money
  - Cause turmoil

Find the targets

- Using public information locate a target
  - Domain name info
    - **Organization:, address:**
    - **Admin contact:, email:, phone:, fax:**
    - **Tech contact:, email:, phone:**
    - **Nameservers:**
  - Web site
    - Gather employee info, remote sites, partnerships, network info
  - Search Engines
    - Search on the target and employees

Locate the target's assets

- Assets
  - Computers
  - Routers
  - Firewalls
  - Dial-in connections
  - Remote sites
  - People

Locate the target’s assets

- Lots of tools to find out about devices
- These are active probes of the network and can be detected
- Some probes are part of normal communications and are hard to detect
- Social Engineering

Find any vulnerabilities in the assets

- OS fingerprinting
- Default password
- Social engineering

NMAP

```
Starting nmap V. 2.54BETA30 www.insecure.org/nmap/ )
The 1537 ports scanned but not shown below are in state: closed)

          21/tcp open ftp                auth 143/tcp open
          22/tcp open ssh                imap2 515/tcp
          25/tcp open smtp               open printer 587/tcp
          80/tcp open http               open submission 993/tcp
          110/tcp open                   open imaps 995/tcp
          pop-3 111/tcp open             open pop3s
           sunrpc 113/tcp open

Remote operating system guess: Linux 2.1.19 - 2.2.17 Uptime 10.015 days
  (since Mon Feb 4 12:15:36 2002)
Nmap run completed -- 1 IP address (1 host up) scanned in 3 seconds
```

Gain access

- Password guessing
  - Social engineering
  - Default password
- Packet sniffing
- Network attacks
  - Redirects
  - Man in the middle
- Buffer overflows
- Trojan horses, viruses, worms

Increasing access

- Once they have gained access now what
- Increase access is done to become the privileged user on a machine
- Use you as a launch point for an attack
  - DDOS
  - IP hiding

Increasing access

- Password cracking
- Known exploits
  - Public tools that can be run to increase access
- Password guessing
- Exploiting trust relationships

Gather data

- Password sniffers
  - ec & others that sniff the networks and email password back to the hacker
- Look for information in the system
  - Other password
  - Memos, letters, confidential info
  - Financial information

Making a backdoor

- Create user accounts
- Modify password to dormant accounts
- Batch jobs
- Replace applications with Trojan applications (secret user/password)

Cover tracks

- Clear log files
- Replace applications (rootkit)
- Blow away entire system

Trashing it or taking it off-line

- Sometimes if the attacker can not gain access they may try to stop access.
- That may also be the goal from the beginning
- This as a Denial of Service Attack (DoS)

DOS & DDOS

- Goal is to take a system or service off-line
- Can be done in as little as one message
- DDOS – multiple attackers
  - Uses hacked computers to launch the attack
  - Very hard to stop.

Why is still a problem?

- If this was a technology issue only we could win.
- Information Assurance is a Social/human issue
- The information war cannot be won on technology alone
- Everyone must be involved

Iowa State Plan

Build a nationally recognized program in Information Assurance

- Education + Research + Outreach
- Interdisciplinary effort

Major IA Components at ISU

- Multidisciplinary Program at Iowa State
- ISU Information Assurance Center
- NSF CyberCorp fellowships
- Graduate education
  - Masters of Science in Information Assurance
  - MS programs specializing in IA in: CprE, CS, Math, PolySci, MIS, and IMSE
  - PhD programs specializing in IA: CprE and CS

Graduate Certificate Program

- Four courses offered via distance education (streaming or video tape)

CprE 530:	Computer Network Protocols
CprE 531:	Computer System Security
CprE 532:	Information Warfare
CprE/Math 533:	Cryptography

Questions

From the art of war

If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.